مجلة كلية الكوت الجامعة Al-Kut Univ. College Journal العدد 1 السنة الأولى 2016
ISSN: 2414 - 7419

Randomly Encryption-Decryption Using Genetic Algorithm and ASCII code

Hind Saleem Ibrahim [1] *Thekra Abbs[2], Eman Saleem Ibrahem [3]

[1] Atmospheric Science, University of Mustansiriyah,[2] Computer Sciences, University of Mustansiriyah, [3]Media Unit and Informatics, University of Baghdad

Abstract

During the last decades, information cryptography has become necessary; this is because the widely use of multimedia document over the net and the necessity of these document to be protected from attacks. A demand for a strong encryption and decryption, which is very hard to crack, made cryptography techniques investigated and developed. In this work, a new encryption/decryption message method by used the genetic algorithms has been presented that preserve the communication channels security via making it hard to attacker to predicate a pattern of the encryption / decryption scheme. This paper proposed a method based on genetic algorithm and ASCII to achieve two levels of security, the first level of security are a key form ASCII code and the second level of security are a key form Genetic algorithm. The genetic algorithm that been used to generate a key make the key complex by the help of random number generator. The key generation will go through a number of process and main criteria for key selection, will be the fitness value of the population. The execution results show a good performance and high security for the suggested method.

Keywords: cryptography, encryption, decryption, genetic algorithms.

عشوائيه التشفير- فك التشفير عن طريق الخوارزميات الجينية ورمز ASCII

هند سليم ابراهيم حربه , ذكرى عباس , ايمان سليم ابراهيم حربه

الخلاصة

خلال العقود الأخيرة، أصبح من الضروري تشفير المعلومات؛ وذلك لاستخدامها على نطاق واسع من الوثيقة الوسائط المتعددة عبر شبكة الإنترنت، وضرورة وجود هذه الوثيقة إلى أن

تكون محمية من الهجمات. والطلب على التشفير القوي وفك التشفير، والتي من الصعب جدا للقضاء على الكراك، وتقنيات التشفير جعل التحقيق فيها وتطويرها. في هذا البحث،تقديم طريقة جديدة للتشفير ورسالة فك التشفير عن طريق الخوارزميات الجينية التي تحافظ على الأمن على قنوات الاتصال التي تجعل من الصعب على المهاجمين التعرف على نمط نظام التشفير / فك التشفير. في هذا البحث تم تقديم طريقة تقوم على الخوارزمية الجينية وكود ASCIIإلى تحقيق مستويات اثنين من الأمن. يعرض أولا المستوى الأول للأمن بشكل رئيسيي على شكل كود ASCII وثانيا المستوى الثاني على شكل الخوارزمية الجينية بصورة رئيسية .حيث تمثل الخوارزمية الجينيةا لتي تستخدم لتوليد مفتاح،وذلك عن طريق توليد الأرقام العشوائية . وأهم معايير الاختيار الرئيسية لتوليد المفتاح من خلال العديد من العمليات ، وسوف تكون قيمة صلاحية المجتمع للسكان.حيث أظهرت النتائج إعداد أداء جيدا وأمان عال للطريقة المقترحة.

1. introduction

Today cryptography which is a part of encryption science plays a main role in many field such as sending private e-mails, e-commerce, mobile phone communication, transmitting financial information, etc. The use of encryption/decryption is as old as the art of communication. In previous time (at war time) cipher was called wrongly as a code, which was employed to prevent the enemy from getting the secret information that transmitted over communication systems.

Data encryption is very important especially when data transmitting through network, which helps to secure these data because it physically difficult to secure all access to networks. After the message received by receptor, he should have a decryption program to returned it to its original readable form. The encryption can give a powerful security for data to provide highest level of security for sensitive data. The encryption goal is to make data vague to receptor and very hard to decipher when attacked. The encrypted data security are depends on many factors such as key size type of encryption algorithm, algorithm implemented in the product, etc.

The encryption process work to translating the secret message (that is in normal form) to an encrypted message that is written with secret characters [1, 2]. Decrypting process is act to translating encrypted message into unencrypted message (readable

message). Genetic algorithms are evolutionary algorithms based on the notion of natural selection [3]. The genetic algorithm has been proved its powerful and reliable optimization technique in a wide range of applications, which can be applied to both images and texts. Nowadays, many papers have proposed encryption and decryption algorithms using genetic algorithms. But most of the proposed algorithms suffered from some problems such as time delay on the network communication channels and lack of robustness.

In the proposed technique a new method for encryption and decryption message via genetic algorithms is presented which maintains the security on the communication by making it difficult for attacker to predicate a pattern of the encryption / decryption scheme by using two levels of security. The idea is to generate two keys for ciphers, first key form ASCII code which presents first level of security and second key form Genetic algorithm which represents second level. Since genetic algorithm does not utilize the natural numbers directly so the result obtained for generating keys in our method was so good in term of cryptography. [4]

This paper is structured as follows: encryption algorithm to generate first key and second key, generate cipher text and cipher message in the second section. Third section include decryption algorithm. Experiment result and result analysis in section four and five and finally, in section 6, the most important conclusions are explained.

2. Encryption Algorithm

In the first stage the Encryption algorithm generates keys that used to encrypt and descript the massage. The suggested algorithm will produced two keys, one from text message and the second from genetic algorithm (the most complicated part of the algorithm). The two keys can be generated as follows:

2.1 The First key

Convert each symbol (character) in the text massage to decimal number which represent the ASCII Code of the character.

2.2 The second key

This step will be done by using simple genetic algorithm to generate second key randomly. The key must not exceed 128 which represent half number of the total character in ASCII (256). In this work, it used simple genetic algorithm.

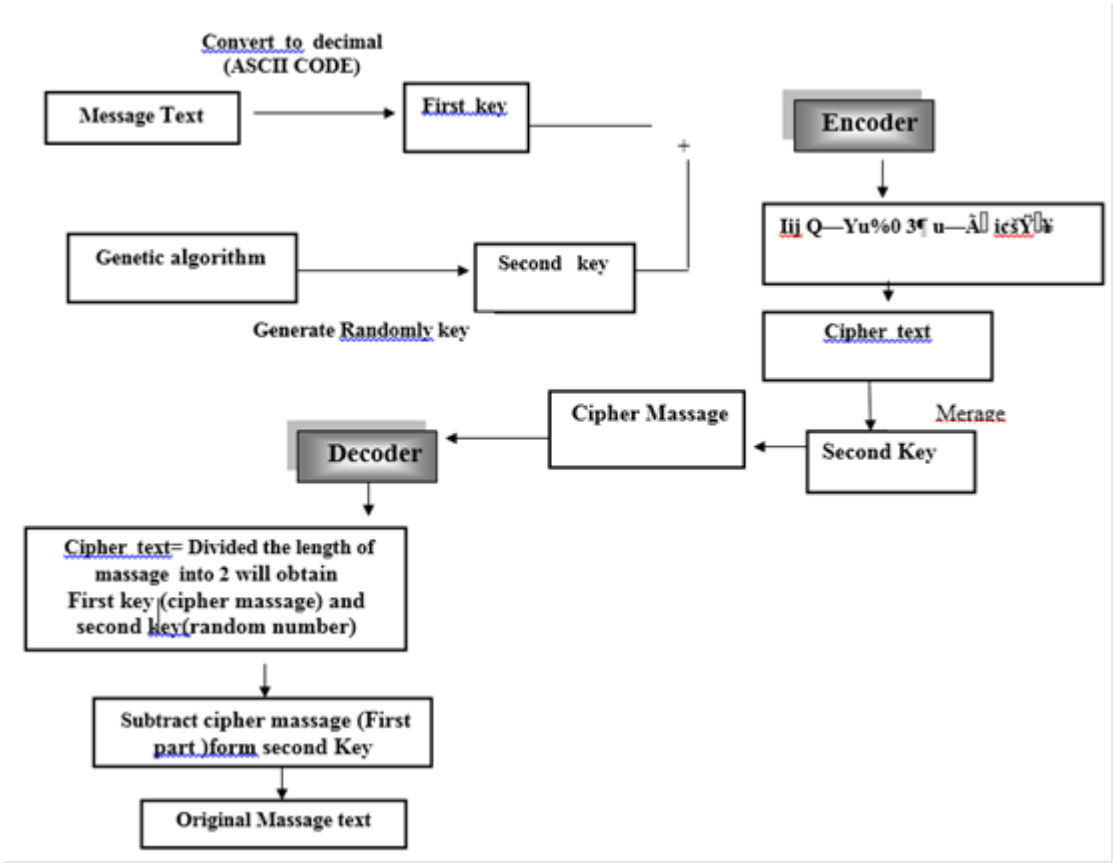


Figure (1) :generic process of encoding and decoding

2.2.1 Generate the chromosome:

We generated a key (chromosome) randomly each gene either 0 or 1, (the random bit generator is either an algorithm or device that outputs a sequence of unbiased binary digits and statistically independent) [5]. The length of the chromosome depend on the number of characters in the message multiply by seven positions which represent one character in ASCII.

2.2.2 Fitness

This part propounds many tests designed for quality measurement to algorithm of random bit generator. As it is unattainable to offer a mathematical substantiation that a generator is truly a random bit generator, the tests depict here are help to detect a proven weaknesses kinds that generator may have [6]. This is achieved by pick a sample generator output sequence and subject it to diffrent statistical tests to specify the possesses of sequence for a certain attribute which is really random sequence. The five statistical tests are:

(i) Frequency test: this test aim to detect if the number of 1's and 0's in s are same approximately, that should be expected from random sequence as shown in equation (1) [5,6,3,11]:

$$x_1 = \frac{(p_0 - p_1)^2}{p} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(1)}$$

Where: p1, p0indicate the 1's and 0's number in s.

(ii) Serial test: the aim of it is to detect if the occurrences number (00, 01, 10, 11) as a subsequences of s are same approximately, that should be expected from random sequence as shown in equation (2)

(iii)

$$x_2 = \frac{4}{p-1}\left(p_{00}^2 + p_{01}^2 + p_{10}^2 + p_{11}^2\right) - \frac{2}{p}\left(p_0^2 + p_1^2\right) + 1 \quad \ldots\ldots\ldots\ldots\ldots \text{(2)}$$

Where: p1, p0 indicate the number of 1's and 0's in s respectively. Note that p00 + p01 + p10 + p11 = (p − 1) due to the subsequences are allowable to overlap [2, 7, 8].

(iv) Poker test: it define if the length sequences f it approximately has the same times number in s that would be expected from random sequence as shown in equation (3) [,2 7, 8, 9].

$$x_3 = \frac{2^f}{k}\left(\sum_{i-1}^{2f} p_i^2\right) - k \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(3)}$$

Where: m is an integer in a positive singe

(v) Run test: this test determine if the runs number (ones or zeros) of diffrent lengths in the sequence s is would be expected from random sequence as shown in equation (4)

$$x_4 = \sum_{i=1}^{k} \frac{(h_i - l_i)^2}{l_i} + \sum_{i=1}^{k} \frac{(j_i - l_i)^2}{l_i} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(4)}$$

Where: li is the length of (i), j_i, h_i number of gaps and blocks respectively, k is the largest integer (i) where where li ≥ 5,

The gaps number (or blocks number) of (i) length that expected in a random sequence with (n) length is:

$$e_i = \frac{(n - i + 3)}{2i} + 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

This test is aim to specify if the runs number of zeros and ones for different lengths is same as what expected for a random sequence. Practically, this run test specify if the oscillation between such substrings is too slow or too fast [2, 6, 7, 10].

(vi) Autocorrelation test: it is checking the correlations between the s sequence and (noncyclic) shifted versions of it. The statistic used is in equation(6) [2, 7, 8, 9]:

$$\chi_5 = 2\left(b(c) - \frac{p-c}{2}\right) / \sqrt{p-c} \quad \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Where: d are a fixed integer, $b(c) = \sum_{i=0}^{p-c-1}$, $1 \le c \le n/2$. Because of the small values of b(c) are as unexpected as large values of b(c), a two-sided test should be used.

2.2.3 Genetic Operators [11, 12, 13]

The following genetic operator are used to increase the security of the key by generate new random key (second key)

1. **Selection:** this operator pick from the population a specified individuals to be the parents, which has been used to generate a new individuals RWS (roulette wheel selection) that select a higher fitness individuals with a higher probability.
2. **Crossover Operator (Uniform Crossover):** from the set selected-parents, the individuals are mated at random and every pair will be created offspring using uniform crossover. As shown in figure 2.

Parent 1	1	0	0	1	0	1
Parent 2	0	1	0	0	1	1

Uniform point crossover →

Offspring 1	0	0	1	0	0	1
Offspring 2	1	1	0	1	1	1

Figure 2. Example of Uniform Crossover.

3. **Mutation:** In this operation two mutation types were used :
   a. The process of mutation switch between two random points. The probability of mutation has to be small. The mutation helps to prevent the algorithm from being stuck in a local optimal point.

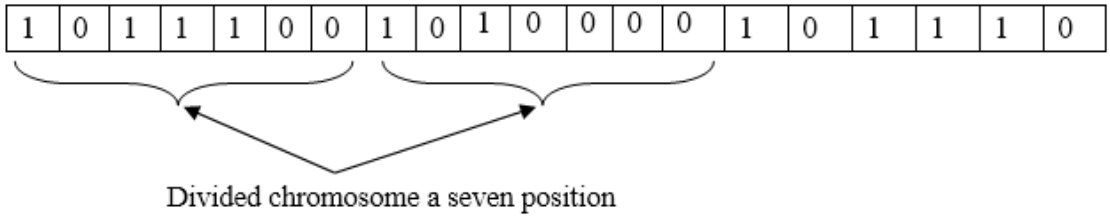
b. Inversion: This is known as the inversion operator [12, 13]. An inversion is select two positions randomly from chromosome and the part of a chromosomes separate from the remnant of the chromosome, after that it change its direction and recombines with the chromosome, as illustrated in Figure 3.

Chromosome
Before Inversion: 010 10100101101010 100
After Inversion: 010 01010110100101 100

Figure 3: The Inversion Operator

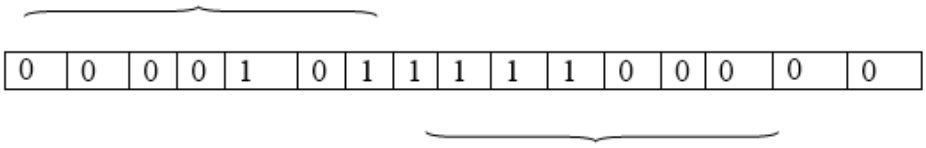
4. **The best individual:** The final fitness function depends on converting the value of chromosome from binary to decimal. Each seven bits separated and convert to decimal. The best individual from algorithm can be selected according to high fitness value, and this represents the second key which obtained from genetic algorithm, for example, the operation of converting binary number to decimal number, as shown in figure 4.

Example:



Divided chromosome a seven position

For example



No1=5, no 2= 112 ….. etc., for remain chromosomes

5	112	144	1	1	0	128	32	2

Figure (4) illustrate the Part of Sample Result of Genetic Algorithm (sample of the best individual)

2.3 Cipher Text

After that the values of the first key (text) and the second key (form GA) are added together then we obtain the cipher text.

2.4 Cipher Message

The cipher text again merges with the second key to obtain the secret message that will be send to the receiver.

3. Decryption Algorithm

1. The recipient will receive the message
2. Divided the length of massage by 2 where first part represents the cipher text and the second part represents the second key that used to decrypt the original message.
3. Subtract the second part of the encrypted message (second key) from the first part (cipher text).
4. The recipient will getting the original text original as shown in table (2).

Table (2) phases decryption method

Deycrption(frist part (cipher text)	106	115	127	96	141	118	100	106	37	124	113	173	103	34	121	109
	112	112	36	247	105	48	120	113	102	102						
-																
Second part(second key)	2	4	8	64	32	1	1	2	5	8	8	64	2	2	2	2
	4	4	4	4	128	4	16	16	16	2						
=original massage	104	111	119	32	109	117	99	104	32	116	105	109	101	32	119	105
	108	108	32	119	101	32	104	97	118	101						

4. Experiment Results

1) The first key:
   The message (how much time will we have) has converted from ASCII to decimal numbers (decimal represent the ASCII code of character)

2) The second key:
   This key was generated from the genetic algorithm as shown in table 1.

3) Cipher text:
   Added" the first key values with the second key giving cipher text that represent message encryption as shown in table 1.

4) Cipher message

   From table 1 we can see that finally the cipher message in decimal has converted to ASCII and send to receiver.

Table (1): show phases encryption method

First key	104	111	119	32	109	117	99	104	32	116	105	109	101	32	119	105
	108	108	32	119	101	32	104	97	118	101						
Second key	2	4	8	64	32	1	1	2	5	8	8	64	2	2	2	2
	4	4	4	4	128	4	16	16	16	2						
Cipher text(first key+second key)	106	115	127	96	141	118	100	106	37	124	113	173	103	34	121	109
	112	112	36	247	105	48	120	113	102	102						
Cipher text mareg second key=massage cipher	106	115	127	96	141	118	100	106	37	124	113	173	103	34	121	109
	112	112	36	247	105	48	120	113	102	102	2	4	8	64	32	1
	1	2	5	8	8	64	2	2	2	2	4	4	4	4	128	4
	16	16	16	2												
Massage cipher	js□`□vdj%|q-g"ympp$÷i0x□xf □@□□ @□□□□□□□□□□□¢□□															

5. Results Analysis and conclusions

This works presents Encryption and Decryption message by Genetic Algorithm, the results demonstrated the using of genetic algorithm to generate encryption key. The generated chromosome length depends on the text length and the key that generated will be change in every once. Subjectively, its note easily to discover any key because the keys are randomly generated by genetic algorithms and that gives a very high security to the encryption process.

It is concluded that the security features of the encryption system are highly optimized using genetic algorithm. Also randomness of two encryption keys ensures the secure transmission of the message over internet. The suggested approach is easy to perform but not easy to discover the encryption keys.

References

1-Sha_ Goldwasser and Mihir Bellare “Lecture Notes on Cryptography “ Cambridge, Massachusetts, August 2001.
12-Robert churchhouse “Codes and ciphers Julius Caesar, the Enigma and the internet “,2004 , cambridge university , http://www.cambridge.org .

2- A. Menezes, P. van Oorschot, and S. Vanstone, This is a Chapter from the Handbook of Applied Cryptography, CRC Press, 1996 . For further information, see www.cacr.math.uwaterloo.ca/hac
3- S., N. Sivanandan, S. N. Deepa, “Introduction to Genetic Algorithm”,Springer Verlag Berlin Heidelberg, 2008.

4- Goldberg, D.E.,”Genetic algorithm in search, optimization, and machine learning “, Addison- Wesley, New York, 1989.

5- A. Tragha, F. Omary, A. Kriouile, ,Genetic Algorithms Inspired Cryptography A.M.S.E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D : Computer Science and Statistics, November 2005

6- A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography,CRC Press, 1996. For further information, see www.cacr.math.uwaterloo.ca/hac

7- Rasheed, Sh. A., "Genetic Algorithms Application in Pattern Recognition", Master's thesis, National Computer Center Higher Education Institute, 2000.

8 -Sindhuja K , Pramela Devi S.,"A Symmetric Key Encryption Technique Using Genetic Algorithm",Department of Computer Science and Engineering,M.V.J College of Engineering, Bangalore, India.

9- Bethany Delman.,"Genetic Algorithms in Cryptography",A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Engineering

10- Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.

11- Bethany Delman.,"Genetic Algorithms in Cryptography", College of Engineering Rochester Institute of Technology Rochester, New York
July 2004

12- D.E.Goldberg,"Genetic Algorithm in search, optimization, and Machine learning", Addison-Wesley, 1989.

13- Lon Riesberg "Genetic Algorithms – New Tools for the Programmers' Toolbox" , April 16, 2003.